# CCSU

## DEPARTMENT OF MATHEMATICAL SCIENCES

# COLLOQUIUM

Friday, December 3
3:00 – 4:00 PM
Maria Sanford, Room 101

# HASH FUNCTIONS AND THE MATH BEHIND CRYPTOCURRENCIES


## ERIK BOSWELL

### CENTRAL CONNECTICUT STATE UNIVERSITY



**Abstract:** Cryptocurrencies have seen a large rise in the past decade. Starting from Bitcoin to having more coins than one could imagine and now coins worth tens of thousands. But how do all of these coins function? What is the driving mathematics behind cryptocurrencies? Hash functions have been around since the 90's presenting very reliable methods of encryption. This discussion will explore the basics of what a hash function is, and the SHA-256 protocol used in bitcoin and many other cryptocurrencies to maintain its security. This will include coverage of hash function properties, Boolean algebra and the SHA-256 algorithm with live examples to see how exactly a hash function behaves.


**To join us online use the following link:**
https://ccsu.webex.com/meet/gotchev


**For further information:**
*gotchevi@ccsu.edu* 860-832-2839
http://www.math.ccsu.edu/gotchev/colloquium/